

# **MAINCRAFTS TECHNOLOGY INTERNSHIP PROGRAM**

## **CYBER SECURITY TASK -2 PERSONAL CYBERSECURITY LAB**

*-Submitted by*

**API AKSHAYA A**

**Intern ID:MT1184**

## 1. Introduction

This report documents the successful setup of a **personal cybersecurity practice lab** in a safe and isolated environment.

The lab is designed for learning basic cybersecurity concepts such as virtualization, network isolation, and web application testing.

---

## 2. Objective

The objective of this task is to:

- Build a safe and isolated cybersecurity lab
  - Set up an attacker machine (Kali Linux)
  - Deploy a vulnerable web application (OWASP Juice Shop)
  - Validate connectivity and basic security tools
- 

## 3. System Requirements

Component	Specification
Operating System	Windows
RAM	8 GB
Disk Space	40 GB free
Virtualization	Enabled
Software	VirtualBox, Kali Linux

---

#### 4. Lab Architecture

The lab consists of:

- **Host System** (Personal Computer)
- **Kali Linux VM** (Attacker)
- **OWASP Juice Shop** (Vulnerable Web Application)
- **Isolated Network Setup**

#### Network Configuration:

- NAT: Internet access
  - Host-Only / Localhost: Internal lab communication
-

## **5. Tools Used**

- VirtualBox
  - Kali Linux
  - Docker
  - OWASP Juice Shop
  - Nmap
  - Burp Suite
- 

## **6. Implementation Steps**

### **Step 1: Kali Linux Setup**

- Kali Linux virtual machine was started successfully.
  - Internet connectivity was verified.
- 

### **Step 2: Target Application Setup**

- Docker was installed and enabled.
- OWASP Juice Shop container was pulled and executed.
- Application was accessed using:

http://localhost:3000

---

### **Step 3: Network Verification**

- IP configuration was verified using:

ip a

---

### **Step 4: Connectivity & Scanning**

- Basic scan was performed using:

nmap localhost

---

### **Step 5: Tool Validation**

- Burp Suite was launched successfully.
  - Web traffic was intercepted to validate proxy configuration.
- 

## **7. Results**

- Kali Linux attacker machine was successfully configured.
- Vulnerable web application was deployed and accessed.

- Network connectivity was verified.
  - Basic security tools functioned as expected.
- 

## 8. Conclusion

This task successfully established a **safe cybersecurity lab environment**.

The lab provides a strong foundation for future tasks such as vulnerability assessment, penetration testing, and incident response practice.

---

## 9. Evidence Attached

- Kali Linux running screenshot
  - OWASP Juice Shop webpage
  - IP configuration output
  - Nmap scan output
  - Burp Suite interface
- 

## 10. References

- OWASP Juice Shop Documentation

- [Kali Linux Official Documentation](#)
- [Docker Documentation](#)